

Claims

1. A network switch comprising;
a memory for storing a first secret fact;
a first port for sending said secret fact to a second switch;
a second port for receiving,
a second-type derivative of said first secret fact from said second switch,
pre-defined information about said second switch, and
a third-type derivative of said pre-defined information about said second switch;
a processor for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said second switch and said third-type derivative of said pre-defined information about said second switch.
2. The switch of claim 1 wherein said first port and said second port are the same port.
3. The switch of claim 1 wherein said comparison, between said first secret fact and said second-type derivative of said first secret fact, includes reversing the derivative nature of said second-type derivative of said first secret fact.
4. The switch of claim 1 wherein said comparison, between said first secret fact and said second-type derivative of said first secret fact, includes creating a second-type derivative of said first secret fact.
5. The network switch of claim 1 wherein said second-type derivative is associated with said second switch.
6. The network switch of claim 1 wherein said third-type derivative is associated with said first switch and said second switch.
7. The network switch of claim 1 wherein said pre-defined information about said second switch comprises encryption key information.
8. The network switch of claim 1 wherein said first secret fact is a random number.
9. The network switch of claim 1 wherein said first secret fact is a nonce.

10. A method of mutually authenticating a first port on a first switch with a second port on a second switch, said first port coupled to said second port by a communication medium that is exclusive to said first port and said second port, the method comprising the steps of:

- sending a first fact from said first port to said second port;
- at said second switch, creating a second-type derivative of said first fact,
- sending said second-type derivative of said first fact from said second port to said first port;
- at said first switch, storing said second-type derivative of said first fact in a first memory;
- sending a second fact from said second port to said first port;
- at said first switch, creating a first-type derivative of said second fact;
- sending said first-type derivative of said second fact from said first port to said second port;
- at said second switch, storing said first-type derivative of said second fact in a second memory;
- sending defined information concerning said first switch from said first port to said second port;
- sending a third-type derivative of said defined information concerning said first switch from said first port to said second port;
- at said second switch, comparing said defined information concerning said first switch with said third-type derivative of said defined information concerning said first switch;
- at said second switch, comparing said first type derivative of said second fact with said second fact;
- sending defined information concerning said second switch from said second port to said first port;
- sending a third-type derivative of said defined information concerning said second switch from said second port to said first port;
- at said first switch, comparing said defined information concerning said second switch with said third-type derivative of said defined information concerning said second switch;
- and
- at said first switch, comparing said second type derivative of said first fact with said first fact.

11. The method of claim 10 wherein the step of comparing said defined information concerning said second switch with said third-type derivative of said defined information concerning said second switch, comprises the substeps of:

reversing the derivation of the third-type derivative of said defined information concerning said second switch; and

comparing the result of said reversal with said defined information concerning said second switch.

12. The method of claim 10 wherein the step of comparing said defined information concerning said second switch with said third-type derivative of said defined information concerning said second switch, comprises the substeps of:

making a third-type derivative of said defined information concerning said second switch; and

comparing the made third-type derivative with the received third-type derivative.

13. The method of claim 10 wherein the step, at said second switch, of creating a second-type derivative of said first fact comprises the sub-steps of:

encoding said first fact to yield an encoded first fact; and

encrypting said encoded first fact.

14. The method of claim 13 wherein said encoding is performed by applying a hash function.

15. The method of claim 13 wherein said encrypting is performed using a private key unique to said second switch.

16. The method of claim 10 wherein said defined information concerning said first switch comprises encryption key information.

17. The method of claim 16 wherein said encryption key information comprises a public key uniquely associated with said first switch.

18. The method of claim 10 wherein said third-type derivative is associated with both said second switch and said first switch.

19. The method of claim 18 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority associated with said first switch and said second switch.

20. The method of claim 19 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority being the manufacturer of either said first switch or said second switch.

21. The method of claim 10 wherein the step, at said second switch, of comparing said defined information concerning said first switch with said third-type derivative of said defined information concerning said first switch, comprises the sub-steps of:

reversing said third-type derivative of said defined information concerning said first switch yielding a reversed third-type derivative; and

comparing said reversed third-type derivative with said defined information concerning said first switch.

22. The method of claim 20 wherein said step of reversing said third-type derivative is performed using a public key uniquely associated with an encryption key authority, said encryption key authority associated with said first switch and said second switch.

23. A method of mutually authenticating a first port on a first switch with a second port on a second switch, the method comprising the steps of:

sending from said first port to said second port, an authentication request command having a payload of a first fact;

sending from said second port to said first port, a request acknowledge command having a payload of a second fact, a second-type derivative of said first fact, defined information concerning said second switch, and a third-type derivative of defined information concerning said second switch; and

sending from said first port to said second port, a confirm authentication command having a payload of a first-type derivative of said second fact, defined information concerning said first switch, and a third-type derivative of defined information concerning said first switch.

24. The method of claim 22 wherein said first fact is a random number.

25. The method of claim 22 wherein said first fact is a nonce.

26. The method of claim 22 wherein said second-type derivative of said first fact is created by a method comprising the sub-steps of:

encoding said first fact to yield an encoded first fact; and

encrypting said encoded first fact.

27. The method of claim 25 wherein said encoding is performed by applying a hash function.

28. The method of claim 25 wherein said encrypting is performed using a private key unique to said second switch.

29. The method of claim 22 wherein said defined information concerning said first switch comprises encryption key information.

30. The method of claim 28 wherein said encryption key information comprises a public key uniquely associated with said first switch.

31. The method of claim 22 wherein said third-type derivative is associated with both said second switch and said first switch.

32. The method of claim 30 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority associated with said first switch and said second switch.

33. The method of claim 30 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority being the manufacturer of either said first switch or said second switch.

34. The method of claim 22 further comprising the step of comparing, at said second switch, said defined information concerning said first switch with said third-type derivative of said defined information concerning said first switch.

35. The method of claim 32 wherein said comparing step comprises the sub-steps of:
reversing said third-type derivative of said defined information concerning said first switch yielding a reversed third-type derivative; and
comparing said reversed third-type derivative with said defined information concerning said first switch.

36. The method of claim 33 wherein said step of reversing said third-type derivative is performed using a public key uniquely associated with an encryption key authority, said encryption key authority associated with said first switch and said second switch.

37. A method of mutually authenticating a first port on a first switch with a second port on a second switch, the method comprising the steps of:

20100623 013100

sending from said first port to said second port, an authentication request command having a payload of a first fact, defined information concerning said first switch, and a third-type derivative of defined information concerning said first switch,

sending from said second port to said first port, a request acknowledge command having a payload of a second fact, a second-type derivative of said first fact, defined information concerning said second switch, and a third-type derivative of defined information concerning said second switch; and

sending from said first port to said second port, a confirm authentication command having a payload of a first-type derivative of said second fact.

38. The method of claim 35 wherein said first fact is a random number.

39. The method of claim 35 wherein said first fact is a nonce.

40. The method of claim 35 wherein said second-type derivative of said first fact is created by a method comprising the sub-steps of:

encoding said first fact to yield an encoded first fact;

encrypting said encoded first fact.

41. The method of claim 38 wherein said encoding is performed by applying a hash function.

42. The method of claim 38 wherein said encrypting is performed using a private key unique to said second switch.

43. The method of claim 35 wherein said defined information concerning said first switch comprises encryption key information.

44. The method of claim 41 wherein said encryption key information comprises a public key uniquely associated with said first switch.

45. The method of claim 42 wherein said third-type derivative is associated with both said second switch and said first switch.

46. The method of claim 43 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority associated with said first switch and said second switch.

47. The method of claim 35 further comprising the step of comparing, at said second switch, said defined information concerning said first switch with said third-type derivative of said defined information concerning said first switch.

48. The method of claim 45 wherein said comparing step comprises the sub-steps of:
reversing said third-type derivative of said defined information concerning said
first switch yielding a reversed third-type derivative; and

comparing said reversed third-type derivative with said defined information
concerning said first switch.

49. The method of claim 46 wherein said step of reversing said third-type derivative
is performed using a public key uniquely associated with an encryption key authority, said
encryption key authority associated with said first switch and said second switch.

50. A method of mutually authenticating a first port on a first switch with a second
port on a second switch, the method comprising the steps of:

receiving on said second port any recognized communication and interpreting said
recognized communication as having a recognized purpose and an additional purpose, said
additional purpose being a request for authentication command;

at said second switch, creating a second-type derivative of said recognized
communication and storing said second-type derivative and said recognized communication in a
memory;

sending from said second port to said first port an acknowledge request command
having a payload of a second fact, said second type derivative of said recognized
communication; defined information concerning said second switch, and a third-type derivative
of defined information concerning said second switch; and

sending from said first port to said second port, a first-type derivative of said
second fact, defined information concerning said first switch, and a third-type derivative of
defined information concerning said first switch.

51. A method of authenticating a first port on a first switch with a second port on a
second switch, the method comprising the steps of:

at said first switch generating a random or pseudo-random first fact;

at said first switch, storing said first fact in a first memory;

sending from said first port to said second port, an authentication request
command;

sending from said first port to said second port, said first fact;

at said second switch, storing said first fact in a second memory;

at said second switch, generating a random or pseudo-random second fact;
sending from said second port to said first port, a request acknowledge command;
sending from said second port to said first port, said second fact, said second switch's PKI certificate, and a signed-first fact comprising a version of said first fact that has been signed using a PKI public key uniquely associated with said second switch;

at said first switch, attempting to verify said second switches PKI certificate using a public key of a certificate authority that is common to both said first switch and said second switch;

at said first switch, attempting to verify said second switches signature using said PKI public key uniquely associated with said second switch;

sending from said first port to said second port, a confirm command;

sending from said first port to said second port, said first switch's PKI certificate, and a signed second fact comprising a version of said second fact that has been signed using a PKI public key uniquely associated with said first switch;

at said second switch, attempting to verify said first switches PKI certificate using said public key of a certificate authority that is common to both said first switch and said second switch; and

at said second switch, attempting to verify said first switches signature using said PKI public key uniquely associated with said second switch.

52. The method of claim 49 wherein said first fact is a nonce.

53. The method of claim 49 wherein said first switch is designated to initiate authentication because it has a higher world-wide name than said second switch.